EXHIBIT B

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
PAULA M. ROACH (254142)
701 B Street, Suite 1700
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
proach@bholaw.com

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW
ERICH P. SCHORK
1 North LaSalle Street, Suite 4600
Chicago, IL 60602
Tel: 312/621-2000
312/641-5504 (fax)
b.barnow@barnowlaw.com
e.schork@barnowlaw.com

THE COFFMAN LAW FIRM
RICHARD L. COFFMAN
First City Building
505 Orleans St., Suite 505
Beaumont, TX 77701
Tel: 409/833-7700
866/835-8250 (fax)
rcoffman@coffmanlawfirm.com

Attorneys for Plaintiffs

SUPERIOR COURT FOR THE STATE OF CALIFORNIA

COUNTY OF ORANGE – CENTRAL JUSTICE CENTER

MAUDIE PATTON, JACQUELINE GOODRIDGE, and VIRGINIA KALDMO, Individually, on behalf of the general public, and on behalf of all others similarly situated,

Plaintiffs,

v.

EXPERIAN DATA CORP., a Delaware corporation; COURT VENTURES, INC., a California corporation; U.S. INFOSEARCH.COM, LLC, an Ohio limited liability company; and DOES 1-10, inclusive,

Defendants.

Case No. 30-2015-00812589-CU-MC-CXC

Assigned for All Purposes to:
Hon. Judge Thierry Patrick Colaw
Dept. CX-105

CLASS ACTION

COMPLAINT FOR EQUITABLE RELIEF

IMAGED FILE

BLOOD HURST & O'REARDON, LLP

00090544

Plaintiffs Maudie Patton, Jacqueline Goodridge, and Virginia Kaldmo (collectively, "Plaintiffs"), individually and on behalf of the general public and all others similarly situated (the "Class Members"), by and through their attorneys, upon personal knowledge as to facts pertaining to them and on information and belief as to all other matters, complain of the actions of Defendants Experian Data Corp. ("Experian"), Court Ventures, Inc. ("CVI"), and U.S. Infosearch.com, LLC ("USI") (collectively, "Defendants"), and respectfully state the following:

NATURE OF THE CASE

1. CVI and USI, and later, Experian and USI, without authorization, sold or granted access to the highly sensitive, confidential, and regulated consumer, financial, and personal records and information, including consumer credit information and Social Security numbers (collectively, "PII"), of 200 million[1] U.S. citizens (*i.e.*, Plaintiffs and Class Members) in the USI/CVI/Experian databases to Hieu Minh Ngo ("Ngo"), a known and now convicted identity thief, black market PII trafficker, and computer hacker, who, in turn, re-sold and granted access to the compromised PII to over 1300 identity theft criminals worldwide for the purpose of engaging in identity theft and identity fraud (the "Security Lapse").

2. Ngo's customers used CVI and Experian to make 3.1 million queries of the USI database over an 18-month period. Access to the compromised PII ended in February 2013, when the CVI/Experian portal used by Ngo and his customers to access the USI/CVI/Experian databases was closed, and the Security Lapse was first revealed. The Security Lapse is one of the most significant and potentially largest data security lapses involving wrongfully disclosed and compromised PII in the history of the United States.

///

[1] According to the U.S. Census Bureau, the U.S. population during 2012, the bulk of the time the Security Lapse took place, was approximately 313 million. Also per the U.S. Census Bureau, approximately 23.3% of the U.S. population was under the age of 18 during 2013. *See* http://quickfacts.census.gov/qfd/states/00000.html (last visited Sept. 6, 2015). Accordingly, during 2012, there were approximately 240 million adults in the U.S. with the type of PII contained in the CVI/USI/Experian databases. Thus, while Ngo's PII portal and black market websites were up and running, Ngo and his fraudster clientele had access to the PII of 83% of the U.S. adult population.

3. This action seeks to require Defendants to notify all victims of the Security Lapse pursuant to various state data breach notification statutes and general principles of equity. Plaintiffs sue Defendants for violating at least 26 state data breach notification statutes. Plaintiffs also seek (i) declaratory relief pursuant to California Code of Civil Procedure ("C.C.P.") §1060; and (ii) an injunction requiring notification of the Security Lapse and other relief under the general principles of equity.

4. Providing notice of the Security Lapse to its actual victims will fulfill the December 18, 2013 representation and promise made to Congress by Tony Hadley, Experian's Senior Vice President of Government Affairs and Public Policy, wherein he stated that "we know who they [the Security Lapse victims] are, and we're going to make sure they're protected." To date – over 18 months later – none of the Defendants have notified the Security Lapse victims or otherwise protected them.[2]

5. Notice of the Security Lapse also will put the victims on notice to be vigilant about their identities and finances, and take to the appropriate remedial and protective measures. Providing notice is not only the right thing to do, but legally mandated. Without individualized notice, Security Lapse victims do not know whether or how their PII was compromised, the categories of PII compromised, and the types of identity theft and identity fraud to which they have been exposed or actually suffered. Notice of the Security also will alleviate concerns and bring peace of mind to individuals whose PII was not sold or made available to Ngo and his fraudster customers by Defendants.

6. As professed experts in data breach management, Defendants know well that the law requires that victims of a data breach, such as the Security Lapse, be notified about the unauthorized disclosure of their PII. As a major purveyor of highly profitable credit

[2] Later, in a March 30, 2014 press release, Gerry Tschopp, Experian's Senior Vice President of Public Affairs and Public Relations, reversed field, claiming that "[i]n terms of notifying consumers, Experian does not know which consumers' information was disclosed as the data did not come from an Experian database and no other information now available to Experian would identify which consumers should be notified." *See* http://www.experian.com/blogs /news/2014/03/30/court-ventures/ (last visited September 6, 2015). Although Tschopp extended Experian's commitment to get to the bottom of the situation (*see id.*), to date, Experian has failed to live up to its commitment.

monitoring and data breach remediation products, Experian also knows the undisputable benefits that credit monitoring, expense reimbursement funds, data breach insurance, and other data breach protection and remediation products provide.

7. Plaintiffs and Class Members are entitled to notification of whether they are (or are not) victims of the Security Lapse. Plaintiffs and Class Members are no less entitled to protection and remediation than the federal employees victimized by the massive data breach at the U.S. Office of Personnel Management ("OPM") in June 2015.[3]

JURISDICTION AND VENUE

8. The Superior Court of the State of California has jurisdiction pursuant to C.C.P. §410.10. Additionally, no plaintiff has a claim that exceeds $75,000 in controversy and the aggregate amount in controversy of all Plaintiffs' and Class members' claims is less than $5 million.

9. This Court has personal jurisdiction over Defendants because they are licensed to do business in the State of California and during the relevant time period, each Defendant did sufficient business in, had sufficient contacts with, and intentionally availed themselves of the laws and markets of California as to render exercise of jurisdiction by California courts permissible. Additionally, Defendants have purposefully availed themselves of the benefits of conducting activities in the State of California by directing activities in the State of California and by causing effects in California by acts done elsewhere.

10. Venue is proper in the Superior Court for the County of Orange, State of California, under C.C.P. §395.5 because the acts complained of herein have taken place within the Count of Orange, California, and because Defendants:

///

---

[3] *See* Bob McGovern, Judges Under Fire, Boston Herald, July 11, 2015 at http://www.bostonherald.com/news_opinion/local_coverage/2015/07/judges_under_fire (last visited July 14, 2015) (reporting that although federal judges victimized by the recent OPM data breach will "automatically receive $1 million of identity theft insurance and access to full-service identity restoration services," they are dissatisfied with the fact that the offered "credit monitoring services are available for only 18 months and none of the services cover family members." According to Administrative Office Director James Duff, "[b]oth the scope and duration of the services concern us, as well as many of our judges and employees. We are voicing our concerns about these issues.").

(a) are authorized to conduct business in this country and have intentionally availed themselves of the laws and markets within this county;

(b) do substantial business in this county; and

(c) are subject to personal jurisdiction in this county.

PARTIES

11. Plaintiff Maudie Patton is a citizen and resident of Roswell, New Mexico. On information and belief, Patton's PII was of the type purchased and accessed by Ngo and his fraudster customers from the USI/CVI/Experian databases via the portal established by Ngo through CVI/Experian utilizing Ngo's black market websites, Superget.info and findget.me. Defendants, individually or in conjunction with their sharing practices, maintain PII on approximately 83% of the adult US population and it is thus more likely to include Patton's PII. Patton is concerned about her PII, finances, credit, and identity and, as such, regularly monitors her credit and financial accounts, and carefully stores and disposes of PII and other documents containing PII.

12. Plaintiff Jacqueline Goodridge is a citizen and resident of Coos Bay, Oregon. On information and belief, Goodridge's PII was of the type purchased and accessed by Ngo and his fraudster customers from the USI/CVI/Experian databases via the portal established by Ngo through CVI/Experian utilizing Ngo's black market websites, Superget.info and findget.me. Defendants, individually or in conjunction with their sharing practices, maintain PII on approximately 83% of the adult US population and it is thus more likely to include Patton's PII. Goodridge is concerned about her PII, finances, credit, and identity and, as such, regularly monitors her credit and financial accounts, and carefully stores and disposes of PII and other documents containing PII.

13. Plaintiff Virginia Kaldmo is a citizen and resident of Amelia, Ohio. On information and belief, Kaldmo's PII was of the type purchased and accessed by Ngo and his fraudster customers from the USI/CVI/Experian databases via the portal established by Ngo through CVI/Experian utilizing Ngo's black market websites, Superget.info and findget.me. Defendants, individually or in conjunction with their sharing practices, maintain PII on

approximately 83% of the adult US population and it is thus more likely to include Patton's PII. Kaldmo is concerned about her PII, finances, credit, and identity and, as such, regularly monitors her credit and financial accounts, and carefully stores and disposes of PII and other documents containing PII.

14. Sales of Patton, Goodridge, and Kaldo's PII were without their knowledge or authorization.

15. Defendant Experian Data Corp. is a Delaware corporation with its principal place of business in Costa Mesa, California. Experian is a wholly-owned subsidiary of Experian plc, a Republic of Ireland company. In March 2012, Experian acquired certain assets and liabilities owned by CVI, including the CVI Database. As a result, Experian became the successor in interest to CVI's assets, business, and related liabilities.

16. Experian is part of a global information services group of companies, providing data and analytical tools to its clients around the world. According to its parent company's website, https://www.experianplc.com (last visited on July 17, 2015), the Experian companies "help businesses to manage credit risk, prevent fraud, target marketing offers and automate decision making" and "help people to check their credit report and credit score, and protect against identity theft."

17. Experian collects information on people, businesses, motor vehicles, insurance, and lifestyle data, including data pertaining to United States citizens and residents. Experian's principal lines of business are credit services, marketing services, decision analytics, and consumer services – with, among other things, a claimed expertise in fraud detection.[4]

---

[4] *See* http://www.experian.com/corporate/areas-of-expertise.html (last visited April 14, 2015) and http://www.experian.com/corporate/fraud-detection.html (last visited April 14, 2015) (recognizing, among other things, that "[f]raud is a huge issue that is on the rise," "[t]here is a constant, ongoing battle between fraudsters and legitimate businesses, particularly in the area of digital security," "[t]here is a high social and financial cost to fraud that impacts both organizations and individuals," and "[h]undreds of fraudulent techniques exist, which include anything from theft of a credit or debit card, tax evasion, claims fraud, advertising goods and services that don't exist, falsifying information, or stealing another's identity for gain.").

Experian also boasts that "[f]raud detection and identity management products or services permeate throughout Experian, enabling companies to detect, monitor and assess the risk of fraud at every stage of their customer relationship" and touts its ability to detect cases

Experian may be served with Summons and a copy of this Class Action Complaint by serving its registered agent for service of process, C.T. Corporation System, 818 West Seventh Street, Second Floor, Los Angeles, California 90017.

18. Defendant Court Ventures, Inc. ("CVI") is a California corporation with its principal place of business in Orange County, California. At all relevant times, CVI was in the business of compiling and distributing public records data, such as criminal records, civil suits and judgments, state tax lien, marriage licenses, death certificates, professional business licenses, and bankruptcy petitions, discharges, and dismissals from over 1,400 state and county record depositories (*i.e.*, the "CVI database"), each of which may contain other PII. In March 2012, Experian plc, through Experian, acquired the CVI database and other assets from CVI. As a result, Experian plc and EDC became the successor in interest to CVI's assets, business, and related liabilities. CVI may be served with Summons and a copy of this Class Action Complaint by serving its President and sole shareholder, Robert L. Gundling, 1211 N. Las Brisas, Anaheim, California 92806.

19. Defendant U.S. Infosearch.com, LLC ("USI") is an Ohio limited liability company with its principal place of business in Whitehall, Ohio. USI is a PII and data broker. According to its website, www.usinfosearch.com, USI helps manage risk and fight fraud by providing quality data to companies, licensed investigators, government agencies, and legal industry professionals – including the type of PII at issue in this case. USI may be served with Summons and a copy of this Class Action Complaint by serving its registered agent for service of process, Marcus A. Martin, 5330 East Main Street, Suite 101, Whitehall, Ohio 43213.

20. Plaintiffs do not know the true names or capacities of defendants sued herein as DOES 1 through 10, inclusive, and will amend their complaint toward the same as soon as ascertained. Plaintiffs are informed and believe, and on that basis allege, that each of the fictitiously named defendants was in some manner legally responsible for unlawful actions, unlawful policies, and unlawful practices complained of herein. Plaintiffs will amend their

---

of fraud, automate fraud risk assessment, predict the likelihood of fraud, reduce may types of fraud, and establish shared fraud detection schemes across multiple organizations in a particular industry. *Id.*

complaint to set forth the true names and capacities of said defendants, along with appropriate charging allegations when the same have been ascertained.

21. On information and belief, at all times mentioned herein, each and every defendant, including Doe defendants, was the owner, agent, principal employee, employer, master, servant, partner, franchiser, or joint-venturer of each of his or her co-defendants, and in doing the actions described below was acting within the scope of his or her authority in such ownership, agency, employment, service, partnership, franchise, or joint venture and with the permission and consent of each co-defendant. Each of said defendants, including Doe defendants, is therefore liable under the law, specifically including, but not limited to, the doctrine of respondeat superior and the law of agency, the acts, omissions, and injuries inflicted upon and likely to be inflicted upon plaintiff and other members as described herein.

FACTS

I. The Ngo Identity Fraud Operation and the Security Lapse.

22. In or around late 2010, Ngo, a Vietnamese hacker, fraudulently posed as a private investigator from Singapore named "Jason Low" "doing business" as "SG Investigators," and contracted with CVI for access to its U.S. consumer PII databases. According to Ngo, SG Investigators was employed by a large company to conduct background checks on job applicants.

23. At all relevant times CVI was in the business of aggregating public record court data, such as criminal records, civil suits and judgments, state tax liens, marriage licenses, death certificates, professional business licenses, and bankruptcy petitions, discharges, and dismissals, each of which may contain other PII. CVI aggregated this data from more than 1,400 state and county record repositories. Its databases, which are owned by Experian, collect data from sources representing more than 80% of the U.S. population.

24. Ngo's relationship with CVI gave him access to more than just CVI's databases. At all relevant times, CVI had a reciprocity agreement with USI, whereby the two entities shared information from, and access to, each other's databases. As such, CVI and USI (and later, Experian) subscribers had complete access to each company's U.S. consumer PII

databases.

25. Because CVI and USI (and later, Experian) openly granted access to each other's subscribers, Ngo and his fraudsters accessed the PII of more than 200 million Americans (*i.e.*, approximately 83% of the U.S. adult population) including, *inter alia*, criminal and civil judgment histories, bankruptcy histories, tax lien histories, professional business licenses, marital status, Social Security numbers, addresses, dates of births, personal vital statistics, and bank information.

26. Ngo, posing as SG Investigators, was one of CVI's biggest clients. Ngo regularly wired CVI $15,000 per month from his bank account in Singapore for access to CVI's and USI's (and later, Experian's) consumer PII databases through his CVI (and later, Experian) account.

27. During July 2010, Ngo started reselling U.S. consumer PII from, and granting access to, the CVI and USI (and later, Experian) consumer PII databases through the known fraudster websites, Superget.info and findget.me, which Ngo created and operated. The Superget.info and findget.me websites were hosted by servers located overseas. Registration was free and anonymous. The websites accepted payment in the form of virtual currency, including Liberty Reserve, which the federal government alleges is responsible for laundering over $6 billion of proceeds from criminal activity.

28. The Superget.info and findget.me websites were user friendly, "interfacing" directly with CVI's (and later, Experian's) databases and serving as consumer PII superhighways. The websites were direct portals to CVI's (and later, Experian's) PII databases and USI's PII databases used by Ngo's fraudster clientele.

29. Superget.info, for example, operated in such a way that a visitor could enter a name and a state of residence of a prospective victim, and obtain other PII relating to the victim from CVI's (and later, Experian's) databases and USI's databases, including the victim's complete name, age, date of birth, address, and Social Security number. A successful hit on a Social Security number or date of birth cost a fraudster approximately $3.00, which Ngo collected. At one time, Superget.info boasted that "[a]bout 99% nearly 100% US people

could be found, more than any sites on the internet now."

30. The Superget.info and findget.me websites had 1,300 customers who paid Ngo nearly $2 million over the relevant period to access CVI's (and later, Experian's) databases and USI's databases containing the PII of 200 million U.S. citizens – a substantial portion of which Ngo remitted to Experian/CVI for the privilege. Over an 18-month period ending in February 2013, Ngo's fraudster customers conducted approximately 3.1 million queries, 1.0 million of which were conducted *after* Experian acquired CVI. Since each query could generate an unlimited number of hits, the actual number of individual consumer PII records obtained and utilized by fraudsters to commit further identity theft and identity fraud could be in the tens of millions – potentially as many as 30 million records. *See* http://krebsonsecurity.com/2014/03/experian-lapse-allowed-id-theft-service-to-access-200-million-consumer-records/ (last visited September 6, 2015).

31. In February 2013, the U.S. Secret Service arrested Ngo. On July 14, 2015, Ngo was sentenced to 13 years in prison for his criminal activity.[5]

II. Experian's and CVI's Involvement in the Security Lapse.

32. In March 2012, Experian bought CVI, including the rights and obligations under CVI's data reciprocity agreement with USI, for $18.3 million.

33. When conducting due diligence prior to the acquisition of CVI, Experian learned several facts that should have alerted it that CVI engaged in, and was connected to, unauthorized and unlawful activity, including Ngo's identity fraud operation. For example, CVI represented to Experian that virtually all of the data it sold was publicly available criminal history information, and thus unregulated. But, Experian later learned prior to the purchase that CVI, in fact, accessed certain personal information and, therefore, was subject to regulation. Prior to acquiring CVI, Experian learned that CVI misrepresented its regulatory compliance regarding such information.

[5] *See* Press Release, U.S. Department of Justice, Vietnamese National Sentenced to 13 Years in Prison for Operating a Massive International Hacking and Identity Theft Scheme (July 14, 2015) at http://www.justice.gov/opa/ pr/vietnamese-national-sentenced-13-years-prison-operating-massive-internation al-hacking-and (last visited July 15, 2015).

34. When conducting due diligence prior to the acquisition of CVI, Experian also discovered that the largest buyer of consumer PII was SG Investigators, a Singapore-based private investigator who made substantial monthly wire transfers from its bank in Singapore in payment for accessing CVI's consumer PII databases.

35. Based on this information, Experian should have further investigated CVI's regulatory compliance, Ngo, and SG Investigators' operations. Had Experian properly performed even the most basic additional investigation of Ngo and SG Investigators, Experian would have discovered Ngo's illegal identity fraud enterprise utilizing CVI's consumer PII databases, and shut it down. Experian, however, intentionally or with reckless disregard failed to do so, stood willingly by, facilitated the illicit operation, and reaped the financial benefits of the acquisition of CVI for another ten months.

36. Shortly after acquiring CVI, Experian learned that CVI was unlawfully obtaining public record information through a practice known as "web scraping." Web scraping is prohibited by many of CVI's public record information sources, but CVI web scraped these sites anyway, in violation of the sites' terms of use. In doing so, CVI created workarounds that sidestepped such websites' technological barriers that were designed to prevent web scraping. Thus, both before and immediately after Experian acquired CVI, it was acutely aware of serious issues with CVI's operations that should have caused Experian to launch a thorough and comprehensive internal investigation of CVI to correct the breaches and violations that had occurred.

37. For almost ten months after Experian acquired CVI, Ngo relatedly paid Experian substantial amounts of money for continued access to a now-expanded treasure trove of consumer PII in the Experian/CVI/USI databases. Experian accepted Ngo's payments "with no questions asked." Approximately 1.0 million database queries were made by Ngo and his fraudster customers during this time, for which, according to Marc Martin, the USI CEO, Experian collected at least $500,000.

38. It was only when the U.S. Secret Service notified Experian in November 2012, about its ongoing investigation of Ngo that Experian began to take action – even though before

this date, Experian was in possession of several facts sufficient to put it on notice of the Security Lapse. For example, by that time, Experian had the logs of Ngo's activity and could have learned that Ngo (for his customers) was inputting millions of names and states of residence in order to obtain Social Security numbers, dates of birth, financial accounts information, and other PII. Experian failed to investigate Ngo further until federal authorities contacted Experian and notified it about their investigation. Even without notice, however, Experian should have monitored its transactions in the normal course of its consumer credit reporting and data brokering business. Its failure to do so resulted in the continuation and expansion of the Security Lapse.

39. Ever since federal authorities forced Experian's hand, Experian has been trying to pass the buck. In a contract dispute pending in California state court, Experian concedes that CVI sold consumer data to Ngo "without having vetted to see if he qualified to obtain such information and Ngo in turn sold this information to many hundreds of identity thieves situated all over the world." Experian admits that as successor in interest to CVI's business, assets, and liabilities, CVI's actions exposed Experian to liability to potential liability, governmental scrutiny, fines, penalties, loss of revenues, and damages.[6] An Experian executive also testified before Congress, admitting that during Experian's "due diligence" of CVI, Experian did not obtain "all of the information necessary to vet" CVI's business activities, including its relationship with Ngo.

III. Security Lapses Lead to Identity Theft and Identity Fraud.

40. Identity theft occurs when a person's PII, such as his or her name, e-mail address, address, Social Security number, billing and shipping addresses, telephone number, and payment card information is used without authorization to commit fraud or other crimes.

41. According to the Federal Trade Commission ("FTC"), "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions" and "any privacy framework should recognize additional harms that might arise from

[6] Cross-Compl. ¶6, *Court Ventures, Inc. v. Experian Data Corp.*, No. 30-2013-00682410-CU-BC-CJC (Cal. Super. Ct. Feb. 28, 2014).

unanticipated uses of data."[7] There "is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute [PII]."[8]

42. In fact, while reflecting on the recent OPM data breach, David Sellers, a spokesman for the Administrative Office of the U.S. Courts, opined that "[i]t is certainly a matter of grave concern, as is the case with any security issue . . . . [I]t is not that different than some kind of a disaster. It is of that proportion. The potential for disaster is humongous."[9]

43. Providing meaningful identity theft monitoring and identity theft insurance are widely recognized as necessary for every person whose PII is taken. For example, the federal government is providing identity theft monitoring, identity theft insurance and restoration services to all 21.5 million victims affected by the OPM data breach.[10] The federal government believes these measures (as well as others) are necessary regardless of who was affected by the data breach.

44. Because Plaintiffs' and Class Members' Social Security numbers were disclosed without authorization, they face an imminent, immediate and continuing increased risk of identity theft and identity fraud – similar to that of the federal judiciary as a result of the recent OPM data breach.

45. Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, releases Identity Fraud Reports quantifying the impact of data security breaches. According to Javelin's 2012 report, individuals whose PII is subject to a reported security breach – such as the Security Lapse at issue here – are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Javelin's most recent

---

[7] FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change*, 8 (March 2012), available at http://www.ftc.gov/os/2012/03/120326privacyreport. pdf (last visited May 8, 2014).

[8] *Id.*: *Comment of Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11–12.

[9] *See* Bob McGovern, *Judges Under Fire*, BOSTON HERALD, July 11, 2015 at http://www.bostonherald.com/news_opinion/local_coverage/2015/07/judges_ under_fire (last visited July 14, 2015).

[10] *See* Information about OPM Cybersecurity Incidents, https//www.opm.gov /cybersecurity, last visited July 16, 2015.

report shows that the total amount stolen in 2013 reached $18 billion. In 2013, one in three people who received data breach notification letters became a victim of fraud, 46% of consumers with breached debit cards became a victim, and 16% of consumers with a breached Social Security number experience fraud.

46. According to the FTC, victims of identity theft and identity fraud are at serious risk of substantial losses. "Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest."[11]

47. Identity thieves use Social Security numbers to commit other types of fraud. The Government Accounting Office (GAO) found that identity thieves use PII to open financial accounts and payment card accounts and incur charges in a victim's name.[12] This type of identity theft can be the most damaging because it may take some time for the victim to become aware of the theft, while in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PII, Social Security numbers are incredibly difficult to change, and their misuse can continue for years into the future.

48. Identity thieves also use Social Security numbers to obtain false identification cards, obtain government benefits in the victim's name, commit crimes, and, as occurred here, file fraudulent tax returns to pilfer the victims' tax refunds. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments, and obtain medical services in the victim's name. Identity thieves also have been known to give a victim's personal information to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record. The GAO states that victims of identity

[11] *See* FTC, *Signs of Identity Theft*, available at http://www.consumer.ftc.gov/articles/0271-signs-identity-theft (last visited July 17, 2015).

[12] *See* Government Accountability Office. *Personal Information*. 9 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (last visited July 17, 2015).

theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."[13]

49. The unauthorized disclosure of a person's Social Security number can be particularly damaging, because Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently, as well as show that he has done all he can to fix the problems resulting from the misuse.[14] Thus, individuals whose PII has been stolen cannot obtain a new Social Security number until the damage has already been done and they have shown they have done all they can to fix the problems.

50. Obtaining a new Social Security number does not absolutely prevent continued identity fraud. Government agencies, private businesses, and credit reporting companies likely still have the person's records under the old number, so the impact of the identity theft may persist long after the incident. For some identity theft victims, a new number may actually create more problems. Because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

51. PII is a valuable commodity to identity thieves. Once PII has been compromised, criminals often trade the information on the "cyber black market" for a number of years.[15] Identity thieves and other cyber criminals openly post stolen credit card numbers, Social Security numbers, and other personal financial information on various Internet websites, thereby making the information publicly available. In one study, researchers found

---

[13] *See* Government Accountability Office. Identity Theft. 2 (PDF pagination) (June 17, 2009) http://www.gao.gov/new.items/d09759t.pdf (last visited July 17, 2015).

[14] *See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327, available at http://www.ssa.gov/pubs/ 10064.html (last visited July 17, 2015).

[15] Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. *See* T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, 3–4 (2009).

hundreds of websites displaying stolen PII. Strikingly, none of these websites was blocked by Google's safeguard filtering mechanism – the "Safe Browsing list." One study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[16]

IV. Defendants Refuse to Notify or Protect the Security Lapse Victims.

52. According to its website, Experian "considers itself a steward of the information it collects, maintains and utilizes. [Its] responsibility is to ensure the security of the information in [its] care and to maintain the privacy of consumers through appropriate, responsible use."[17]

53. Experian further promises on its website that "[w]e use a variety of security systems to safeguard the information we maintain and provide;" and "[w]e maintain physical security for our facilities and limit access to critical areas; and we conduct approval processes before information Experian maintains can be accessed or changed."[18]

54. The Security Lapse has revealed these assurances to be untrue. And, even though Experian considers itself a steward of consumer reports, Experian has not notified the consumers affected by the Security Lapse, or provided them with protection – such as credit monitoring – despite the ethical, moral, and legal requirement to do so. Neither have CVI and USI.

55. After being alerted to the Ngo identity fraud operation, Experian continued its tangled web of contradictions. In a March 30, 2014 Experian press release, Gerry Tschopp, Experian's Senior Vice President of Public Affairs and Public Relations, stated that "[i]n terms of notifying consumers, Experian does not know which consumers' information was disclosed

---

[16] StopTheHacker, *The "Underground" Credit Card Blackmarket*, *available at* http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-black market/ (last visited July 17, 2015).

[17] "Our Approach to Privacy", https://www.experian.com/privacy/ (last visited July 16, 2015).

[18] "Upholding Our Information Values", http://www.experian.com/privacy /information_values.html (last visited July 16, 2015).

as the data did not come from an Experian database and no other information now available to Experian would identify which consumers should be notified." Experian's resources, technological capabilities, line of business (including data breach management and business consulting), and statements by another senior executive suggests that Tschopp's statement is not true. In any event, although Tschopp extended Experian's commitment to get to the bottom of the situation (*see id.*), to date, Experian has failed to live up to its commitment. So have CVI and USI.

56. For example, at a December 18, 2013 hearing of the Senate Committee on Commerce, Science, and Transportation addressing possible legislation concerning the use of consumer information for marketing purposes, Tony Hadley, Experian's Senior Vice President of Government Affairs and Public Policy, testified, under oath, about the Ngo identity fraud victims, stating "we know who they are, and we're going to make sure they're protected."[19] Senator McCaskill expressed concern that the Security Lapse demonstrated that Experian is not a capable steward of the consumer information it collected and shared for marketing purposes. More importantly, and setting aside the fact that Hadley's statement directly contradicts Tschopp's statement, Experian has not made good on Hadley's promise.

57. Consistent with Hadley's statement, Experian's allegations in its cross-complaint against Court Ventures in the California state court litigation indicate that the PII sold by Experian and CVI to Ngo and his fraudster customers is readily ascertainable by Experian. Experian specifically alleges:

> It was only as a result of [the U.S. Secret Service contacting Experian] that Experian had any reason to look at the actual logs for SG Investigators' queries, at which point Experian discovered that SG Investigators was inputting names and states in order to obtain consumers' social security numbers.[20]

///

---

[19] Congressional Hearing Commerce, Science, and Transportation Committee, available at http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=a5c3a62c-68a6-4735-9d18-916bdbbadf01&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a at 2:22:30.

[20] Cross-Compl. ¶18, *Court Ventures, Inc. v. Experian Data Corp.*, No. 30-2013-00682410-CU-BC-CJC (Cal. Super. Ct. Feb. 28, 2014).

The fact that Experian is able to ascertain the identity of the victims of the Ngo identity fraud operation from its logs through reasonable efforts confirms that any pretext for Experian's failure and refusal to provide notice to, and credit monitoring for, the Security Lapse victims is false.

58. Experian's failure and refusal to do so is particularly egregious in light of its self-touted expertise in data breach management. Indeed, Experian's Data Breach Response Guide emphasizes the importance of implementing an effective notification program.[21] Experian's failure to take its own advice to rectify a serious situation that it created, is willful. Its conduct shouts the maxim, "Physician, heal thyself."[22]

59. Defendants' failure and refusal to safeguard and protect Plaintiffs' and Class Members' PII, notify them about the Security Breach, and provide them with protection after Experian promised Congress it would do so has caused (and will continue to cause) Plaintiffs and Class Members to suffer injury and harm and has deprived Plaintiffs and the Class Members of what Congress would have mandated or otherwise provided by for that misdirection.

CLASS ACTION ALLEGATIONS

60. Plaintiffs seek certification of a Class asserting Count I individually on behalf of the following Nationwide Class of similarly situated individuals:

> All persons whose personally identifiable information (PII) was contained in the Experian/CVI/USI databases and subject to being accessed, whether directly or indirectly, through Hieu Minh Ngo's websites, Superget.info and findget.me, from July 1, 2010 to and including February 28, 2013.

61. Plaintiff Jacqueline Goodridge also brings this action as a class action, asserting Count II individually, and on behalf of the following State Data Breach Notification Statute Sub-Class consisting of similarly situated citizens of the States of Alaska, California, Colorado, Delaware, Georgia, Hawaii, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland,

---

[21] *See* Data Breach Response Guide 13 (2014), available at http://www.experian.com/assets/data-breach/brochures/2014-2015-data-breach-response-guide.pdf (last visited July 16, 2015).

[22] LUKE 4:23 (King James).

Michigan, Montana, New Hampshire, New Jersey, North Carolina, North Dakota, Oregon, South Carolina, Tennessee, Virginia, Washington, Wisconsin and Wyoming, and the District of Columbia:

> All persons whose personally identifiable information (PII) was contained in the Experian/CVI/USI databases and subject to being accessed, whether directly or indirectly, through Hieu Minh Ngo's websites, Superget.info and findget.me, from July 1, 2010 to February 2013.

62. Excluded from the Nationwide Class and the State Data Breach Notification Statute Sub-Class are (i) Defendants and their owners, officers, directors, employees, agents, representatives, parent companies, subsidiaries, affiliates, successors, and assigns; and (ii) the Court, Court personnel, and members of their immediate families.

63. This action is properly brought as a class action for the following reasons:

64. The Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members number in the millions and, as such, are so numerous and geographically dispersed that their joinder would be impracticable. The precise numbers of Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members are presently unknown to Plaintiffs, but may be ascertained from Defendants' records. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

65. Common questions of law and fact exist as to all Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members. These questions, which arise from defendants' common course of conduct, predominate over any questions affecting only individual Class members. Among these common questions of law and fact are:

(i) whether Defendants failed to safeguard and protect Plaintiffs' and the Nationwide Class Members' and State Data Breach Notification Statute Sub-Class Members' PII;

(ii) whether Defendants failed to notify Plaintiffs and the Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members whose PII was accessed and/or obtained without authorization in the Security Lapse;

///

(iii) whether Defendants violated applicable state data breach notification statutes by failing to notify Plaintiffs and the Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members whose PII was accessed and/or obtained without authorization in the Security Lapse;

(iv) whether Defendants' failure to notify caused or aggravated Plaintiffs' and the Nationwide Class Members' and State Data Breach Notification Statute Sub-Class Members' injuries and harm; and

(v) whether and to what extent Plaintiffs and the Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members are entitled to declaratory and injunctive relief.

66. Plaintiffs' claims are typical of the Nationwide Class Members' and State Data Breach Notification Statute Sub-Class Members' claims in that Plaintiffs' claims and the Nationwide Class Members' and State Data Breach Notification Statute Sub-Class Members' claims all arise from Defendants' uniform wrongful actions, inaction and omissions, and willful misconduct; to wit, Defendants' failure and refusal to (i) safeguard and protect Plaintiffs' and the Nationwide Class Members' and State Data Breach Notification Statute Sub-Class Class Members' PII; and (ii) properly notify Plaintiffs and the Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members about the Security Lapse.

67. Plaintiffs and their counsel will fairly and adequately represent the Nationwide Class Members' and State Data Breach Notification Statute Sub-Class Members' interests. Plaintiffs have no interests antagonistic to, or in conflict with, the Nationwide Class Members' and State Data Breach Notification Statute Sub-Class Members' interests. Plaintiffs' attorneys are highly experienced in prosecuting consumer class actions and data security breach class actions, and will vigorously prosecute this action on behalf of Plaintiffs and the Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members.

68. This class action is superior to other available methods for the fair and efficiency adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for Class members to prosecute their claims individually. Moreover, the trial and the litigation of Plaintiffs' claims are manageable.

///

69. Defendants have acted, or refused to act, on grounds generally applicable to the Nationwide Class and State Data Breach Notification Statute Sub-Class, thereby making appropriate final injunctive relief and declaratory relief with respect to the Nationwide Class and State Data Breach Notification Statute Sub-Class as a whole.

CLAIMS FOR RELIEF AND CAUSES OF ACTION

COUNT I

INJUNCTIVE RELIEF

(Against all Defendants by the Nationwide Class)

70. The preceding factual statements and allegations are incorporated by reference.

71. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, the resulting Security Lapse, and subsequent nondisclosures have caused (and will continues to cause) Plaintiffs and the Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members to suffer actual and imminent irreparable injury and harm in the form of Defendants' failure and refusal to notify them about the Security Lapse, so they can take the appropriate measures to protect themselves from the immediate and continuing increased risk of identity theft, identity fraud, and other injury and harm. Such irreparable harm will not cease unless and until enjoined by this Court.

72. Plaintiffs and the Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members, however, have no adequate remedy at law other than injunctive relief – to which they are entitled under general principles of equity. There is a substantial likelihood Plaintiffs will succeed on the merits as it undisputed (and indisputable) that the Security Lapse occurred and none of the Defendants have notified any person anywhere that their PII was wrongfully disclosed and compromised or provided the victims with future identity theft or identity fraud protection. The only action Defendants have taken pertaining to the Security Lapse is to point fingers and blame each other for the Security Lapse, all the while keeping the financial benefits reaped from the wrongful sales of Plaintiffs' and the Nationwide Class Members' and State Data Breach Notification Statute Sub-Class Members' PII. Meanwhile, Plaintiffs and the Nationwide Class Members and State Data

Breach Notification Statute Sub-Class Members, and their interests, have fallen through the cracks; Defendants hope they quietly go away.

73. Under general principles of equity, therefore, Plaintiffs and the Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members are entitled to injunctive relief and other appropriate affirmative relief including, *inter alia*, an order compelling Defendants to, *inter alia*, (i) notify each person whether their PII was actually obtained (or not obtained) by Ngo and/or his fraudster customers, (ii) provide three years of credit monitoring and other identity theft and identity fraud protection services to each such person whose PII was actually obtained by Ngo and/or his fraudster customers, (iii) establish a fund (in an amount to be determined) to which such persons may apply for reimbursement of the time and out-of-pocket expenses they incurred to remediate identity theft and/or identity fraud (*i.e.*, data breach insurance), from July 1, 2010 forward to the date the above-referenced credit monitoring terminates; and (iv) refund (or disgorge) their gross revenue from transactions with Ngo and his fraudster customers involving Plaintiffs' and the Nationwide Class Members' and State Data Breach Notification Statute Sub-Class Members' PII and the earnings on such gross revenue.

74. The hardship to Plaintiffs and the Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members if an injunction does not issue substantially exceeds the hardship to Defendants if an injunction is issued. Without proper notification of whether their PII was disclosed and compromised in the Security Lapse, Plaintiffs and millions of Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members will not know whether to take the appropriate measures to protect themselves from identity theft, identity fraud, and other injury and harm. On the other hand, and setting aside the fact that Defendants have the pre-existing legal obligation to employ adequate customer data security measures, Defendants' cost to comply with the above-described injunction, which they are already required to do by state data breach statutes, is relatively minimal. The injury and harm Plaintiffs and the Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members have suffered (and will continue to face) far outweighs any

financial injury Defendants would sustain as a result of the injunctive relief – which Defendants are required by law to do anyway.

75. Issuance of the requested injunction would not adversely affect public policy or the public interest. To the contrary, such an injunction would benefit the public. The PII of up to 83% of the U.S. adult population could have been wrongfully disclosed and compromised by the Security Lapse. Requiring Defendants notify to those persons impacted by the Security Lapse will allow the victims to take the appropriate measures to protect themselves from identity theft, identity fraud, and other injury and harm which, in turn, will benefit the economy and society as a whole. The requested injunctive relief also will hold Defendants accountable for their wrongful actions, inaction, omissions, want of ordinary care, the resulting Security Lapse, and subsequent nondisclosures under the rule of law.

COUNT II

BREACH OF STATE DATA BREACH NOTIFICATION STATUTES

(Against all Defendants by the State Data Breach Notification Statute Sub-Class)

76. The preceding factual statements and allegations are incorporated by reference.

77. Legislatures in the states listed below have enacted data breach notification statutes, which generally require all persons and businesses conducting business within such states that own or license computerized data containing PII to disclose to all residents of the state any data breach of such computerized data by which their PII was acquired by an unauthorized person. These statutes require the disclosure of data breaches to be made expediently and without unreasonable delay.

78. The Security Lapse constituted a breach of Defendants' computer systems within the meaning of the below-listed state data breach notification statutes, which covered and protected Plaintiff Jacqueline Goodridge's and the State Data Breach Notification Statute Sub-Class Members' wrongfully disclosed and compromised PII.

79. Even though Defendants have long since admitted the Security Lapse occurred, and despite Experian's (later quietly retracted) representation to Congress that "we know who

they [the Security Lapse victims] are, and we're going to make sure they're protected," to date, Defendants have failed and refused to notify Plaintiff Jacqueline Goodridge and the State Data Breach Notification Statute Sub-Class Members about the Security Lapse, and the wrongful and unauthorized disclosure of their PII, in violation of the following state data breach notification statutes (as enforced through state consumer protection statutes, where applicable and as noted):

(i) ALASKA STAT. ANN. §45.48.010(a), *et seq.*, as enforced through ALASKA STAT. ANN. §§45.50.471-45.50.561;

(ii) CAL. CIV. CODE §1798.83(a), *et seq.*;

(iii) COLO. REV. STAT. ANN. §6-1-716(2), *et seq.*;

(iv) DEL. CODE ANN. TIT. 6 §12B-102(a), *et seq.*;

(v) D.C. CODE §28-3852(a), *et seq.*;

(vi) GA. CODE ANN. §10-1-912(a), *et seq.*;

(vii) HAW. REV. STAT. §487N-2(a), *et seq.*;

(viii) ILL. COMP. STAT. ANN. 530/10(a), *et seq.*, as enforced through the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILL. COMP. STAT. ANN. §505/2, *et seq.*;

(ix) IOWA CODE ANN. §715C.2(1), *et seq.*;

(x) KAN. STAT. ANN. §50-7a02(a), *et seq.*;

(xi) KY. REV. STAT. ANN. §365.732(2), *et seq.*;

(xii) LA. REV. STAT. ANN. §51:3074(A), *et seq.*;

(xiii) MD. CODE ANN., COMMERCIAL LAW §14-3504(b), *et seq.*, as enforced through Title 13 of the Maryland Consumer Protection Act;

(xiv) MICH. COMP. LAWS ANN. §445.72(1), *et seq.*;

(xv) MONT. CODE ANN. §30-14-1704(1), *et seq.*, as enforced through MONT. CODE ANN. §30-14-103;

(xvi) N.H. REV. STAT. ANN. §359-C:20(1)(a), *et seq.*;

(xvii) N.J. STAT. ANN. §56:8-163(a), *et seq.*, as enforced through N.J. STAT. ANN. §56:8-1, *et seq.*;

(xviii) N.C. GEN. STAT. ANN. §75-65(a), *et seq.*, as enforced through N.C. GEN. STAT. ANN. §75-1.1;

(xix) N.D. CENT. CODE ANN. §51-30-02, *et seq.*, as enforced through N.D. CENT. CODE ANN. CH. 51-15;

(xx) OR. REV. STAT. ANN. §646A.604(1), *et seq.*;

(xxi) S.C. CODE ANN. §39-1-90(A), *et seq.*;

(xxii) TENN. CODE ANN. §47-18-2107(b), *et seq.*;

(xxiii) VA. CODE. ANN. §18.2-186.6(B), *et seq.*;

(xxiv) WASH. REV. CODE ANN. §19.255.010(1), *et seq.*;

(xxv) WIS. STAT. ANN. §134.98(2), *et seq.*; and

(xxvi) WYO. STAT. ANN. §40-12-502(a), *et seq.*

80. Plaintiff Jacqueline Goodridge and the State Data Breach Notification Statute Sub-Class Members suffered injury and harm as a direct or proximate result of Defendants' failure and refusal to provide them with timely and accurate notice of the Security Lapse as required by the above-listed state data breach notification statutes. Had Defendants provided such timely and accurate notice, Plaintiff Jacqueline Goodridge and the State Data Breach Notification Statute Sub-Class Members could have taken the appropriate measures to protect themselves from identity theft, identity fraud, and other injury and harm that may, in fact, already have occurred.

81. On information and belief, no law enforcement agency has informed Defendants that notifying Plaintiff Jacqueline Goodridge and the State Data Breach Notification Statute Sub-Class Members about the Security Lapse would impede any investigation, nor did any law enforcement agency direct Defendants not to make such notification.

82. Plaintiff Jacqueline Goodridge and the State Data Breach Notification Statute Sub-Class Members seek an order requiring that notice of the breach be provided in accordance with these statutes.

///

COUNT III

DECLARATORY RELIEF

(On Behalf of Nationwide Class Against All Defendants)

83. The preceding factual statements and allegations are incorporated by reference.

84. An actual controversy, over which this Court has jurisdiction, now exists between Plaintiffs, State Data Breach Class Members, and Defendants concerning their respective rights, duties and obligations for which Plaintiffs desire a declaration of rights with regard to Defendants' obligation to comply with the state notice statutes identified in paragraph 77 above. Specifically, Plaintiffs and State Data Breach Class Members contend that Defendants have an obligation to provide notice under the notice statutes with which they have not complied.

85. Plaintiffs request a declaration of rights and obligations pursuant to California Civil Code §1060 of Plaintiffs and the State Data Breach Class, on the one hand, and Defendants, on the other, with regard to Defendants' obligation to comply with the state notice statutes.

TOLLING OF THE STATUTES OF LIMITATION

86. The preceding factual statements and allegations are incorporated by reference.

87. **FRAUDULENT CONCEALMENT.** Defendants took active steps to conceal their above-described wrongful actions, inaction, omissions, want of ordinary care, the resulting Security Lapse, and subsequent nondisclosures. The details of Defendants' efforts to conceal their above-described unlawful conduct are in their possession, custody, and control, to the exclusion of Plaintiffs, and await further discovery. When this material information was revealed to Plaintiffs, they exercised due diligence by investigating the situation, retaining counsel, and pursuing their claims. Defendants fraudulently concealed their above-described wrongful conduct. Should such be necessary, therefore, all applicable statutes of limitation (if any) are tolled under the fraudulent concealment doctrine.

88. **EQUITABLE ESTOPPEL.** Defendants took active steps to conceal their above-described wrongful actions, inaction, omissions, want of ordinary care, the resulting Security

Lapse, and subsequent nondisclosures. The details of Defendants' efforts to conceal their above-described unlawful conduct are in their possession, custody, and control, to the exclusion of Plaintiffs, and await further discovery. When this material information was revealed to Plaintiffs, they exercised due diligence by investigating the situation, retaining counsel, and pursuing their claims. Defendants intentionally concealed their above-described wrongful conduct. Should such be necessary, therefore, all applicable statutes of limitation (if any) are tolled under the doctrine of equitable estoppel.

89. **EQUITABLE TOLLING.** Defendants took active steps to conceal their above-described wrongful actions, inaction, omissions, want of ordinary care, the resulting Security Lapse, and subsequent nondisclosures. The details of Defendants' efforts to conceal their above-described unlawful conduct are in their possession, custody, and control, to the exclusion of Plaintiffs, and await further discovery. When this material information was revealed to Plaintiffs, they exercised due diligence by investigating the situation, retaining counsel, and pursuing their claims. Defendants intentionally concealed their above-described wrongful conduct. Should such be necessary, therefore, all applicable statutes of limitation (if any) are tolled under the doctrine of equitable tolling.

PRAYER

WHERFORE, Plaintiffs, for themselves and the Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members, respectfully request that (i) Defendants be cited to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii) Plaintiffs be designated the Class and Sub-Class Representatives; and (iv) Plaintiffs' counsel be appointed Class and Sub-Class Counsel. Plaintiffs, for themselves and the Nationwide Class Members and State Data Breach Notification Statute Sub-Class Members, further request that upon final trial or hearing, judgment be awarded against Defendants, in Plaintiffs' favor for:

(i) injunctive and declaratory relief (as set forth above);

(ii) attorneys' fees, litigation expenses, and costs of suit incurred through the trial and any appeals of this case; and

(iii) such other and further relief the Court deems just and proper.

JURY DEMAND

Plaintiffs, individually and on behalf of the Nationwide Class and State Data Breach Notification Statute Sub-Class, respectfully demand a trial by jury on all of their claims and causes of action so triable.

Dated: September 30, 2015

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
PAULA M. ROACH (254142)

By: *s/ Timothy G. Blood*
TIMOTHY G. BLOOD

701 B Street, Suite 1700
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
proach@bholaw.com

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW
ERICH P. SCHORK
1 North LaSalle Street, Suite 4600
Chicago, IL 60602
Tel: 312/621-2000
312/641-5504 (fax)
b.barnow@barnowlaw.com
e.schork@barnowlaw.com

THE COFFMAN LAW FIRM
RICHARD L. COFFMAN
First City Building
505 Orleans St., Suite 505
Beaumont, TX 77701
Tel: 409/833-7700
866/835-8250 (fax)
rcoffman@coffmanlawfirm.com

Attorneys for Plaintiffs

SHORT TITLE: Patton v. Experian Data Corp.	CASE NUMBER:

Ben Barnow, Barnow and Associates, P.C., 1 North LaSalle Street, Suite 4600, Chicago, IL 60602
Erich P. Schork, Barnow and Associates, P.C., 1 North LaSalle Street, Suite 4600, Chicago, IL 60602
Richard L. Coffman, The Coffman Law Firm, 505 Orleans Street, Suite 505, Beaumont, TX 77701

(Required for verified pleading) The items on this page stated on information and belief are *(specify item numbers, not line numbers)*:

This page may be used with any Judicial Council form or any other paper filed with the court.

Form Approved by the Judicial Council of California MC-020 [New January 1, 1987]

ADDITIONAL PAGE
Attach to Judicial Council Form or Other Court Paper

CRC 201.501